УДК 621.38:004.03

В.С. ПОХИЛ, А.В. ХАРЫБИН

ПАО «Научно-производственное предприятие «Радий», Украина

МЕТОДЫ АНАЛИЗА, ОЦЕНИВАНИЯ И ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ БОРТОВЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ ЛЕТАТЕЛЬНЫХ АППАРАТОВ НА ОСНОВЕ ФУНКЦИОНАЛЬНО-АРХИТЕКТУРНОГО МОДЕЛИРОВАНИЯ

Рассматривается подход к созданию методологического аппарата анализа, оценивания и обеспечения функциональной безопасности авиационных бортовых информационно-управляющих систем на основе ранее разработанных моделей и методов, позволяющих на ранних этапах жизненного цикла БИУС ЛА проводить оценивание и прогнозирование возможных вариантов функционирования БИУС ЛА с поддержанием заданного уровня их функциональной безопасности. Предлагается использовать функционально-архитектурные модели при обосновании распределения вычислительных ресурсов бортовых информационно-управляющих систем по входящим в их состав подсистемам с учетом необходимого уровня надежности и функциональной безопасности.

Ключевые слова: *метод, функциональная безопасность, функционально-архитектурная модель, бортовая информационно-управляющая система.*

Введение

Актуальность. Безопасность и надежность современных летательных аппаратов (ЛА) определяется аналогичными свойствами бортовых информационно-управляющих систем (БИУС), которые в общем случае, представляют собой человеко-машинные системы, базирующиеся на информационно-вычислительных электронных и электрических подсистемах, обеспечивающих автоматизацию всех информационных и управляющих процессов. В БИУС ЛА используются вычислительные подсистемы, представленные совокупностью вычислительных модулей (ВМ) различных подсистем БИУС ЛА, специализированных процессоров (контроллеров) и операционных систем (ОС) реального времени. Эффективность функционирования БИУС ЛА определяется функциональной безопасностью (ФБ), надежностью и производительностью вычислительной подсистемы, которая является неотъемлемой и наиболее важной составляющей современной БИУС ЛА. Одной из задач, которые решаются в вычислительной подсистеме (ядре) БИУС ЛА является формирование управляющих команд, в том числе в условиях возникновения отказов в подсистемах БИУС ЛА. Отказ оборудования, нарушения в работе программного обеспечения, а также неквалифицированные действия экипажа могут стать причиной аварии ЛА с катастрофическими последствиями поэтому вычислительная подсистема перспективной БИУС ЛА должна осуществлять непрерывный мониторинг и анализ состояния оборудования ЛА, и, в случае возникновения отказов, осуществлять эффективное перераспределение (реконфигурацию) оставшихся вычислительных ресурсов, с учетом критичности (важности) процессов и требований к их надежности и безопасности. В случае проявления серии отказов, приводящих к ситуации, при которой нет возможности обеспечить выполнение всех необходимых для штатного функционирования всех подсистем БИУС процессов, она должна обеспечить функционирование тех функциональных подсистем, которые обеспечивают безопасность (связаны с безопасностью) полета ЛА.

Анализ литературы. В статье [1] предложен метод анализа и оценки ФБ БИУС ЛА, позволяющий учесть критичность отказов отдельных элементов БИУС ЛА, выполняющих функции безопасности ($F_Б$), и структурную надежность рассматриваемых подсистем БИУС ЛА. В статьях [2, 3] описаны методы обеспечения необходимого уровня ФБ БИУС ЛА на этапе их проектирования и эксплуатации, позволяющие учесть степень критичности отдельных элементов структурно-фукциональной схемы БИУС и ее реальное состояние, используя возможность структурно-архитектурной реконфигурации вычислительного ядра (ВЯ) БИУС ЛА и перераспределения вычислительных ресурсов в нем. В статье [4] предложена и рассмотрена функционально-архитектурная модель БИУС ЛА, имеющей возможность реконфигурации ВЯ.

Целью статьи является описание комплексного подхода к анализу, оценке и обеспечению функциональной безопасности БИУС ЛА на основе описанных в статьях [1-4] методов и моделей, а также описание применения функционально-архитектурной модели БИУС ЛА при реализации данного подхода.

1. Постановка задачи исследования

Ввиду отсутствия единого методологического аппарата анализа, оценивания и обеспечения функциональной безопасности БИУС ЛА, предлагается комплексный подход к оцениванию значений показателей, характеризующих функциональную безопасность (ФБ) БИУС ЛА и обеспечению их на уровне, который характеризует безопасное состояние ЛА используя ранее предложенные методы анализа, оценивания и обеспечения ФБ на различных этапах жизненного цикла данного класса систем.

В статье [4] функционирование БИУС ЛА было предложено описывать с помощью функционально-архитектурной модели, которая должна описывать распределения ограниченных ресурсов вычислительной подсистемы БИУС ЛА для поддержки наиболее важных (критических) процессов с обеспечением их функционирования с заданной надежностью. В данной статье описано решение задачи разработки модели управления распределением ограниченных ресурсов вычислительной подсистемы БИУС ЛА при обеспечении требуемого уровня надежности и ФБ выполнения функций безопасности в подсистемах БИУС ЛА.

2. Подход к созданию методологического аппарата анализа, оценивания и поддержания функциональной безопасности БИУС ЛА

Взаимосвязь методов и моделей, составляющих методологический аппарат позволяющий осуществлять анализ, оценивания и обеспечение уровня функциональной безопасности БИУС ЛА приведен на рис. 1.

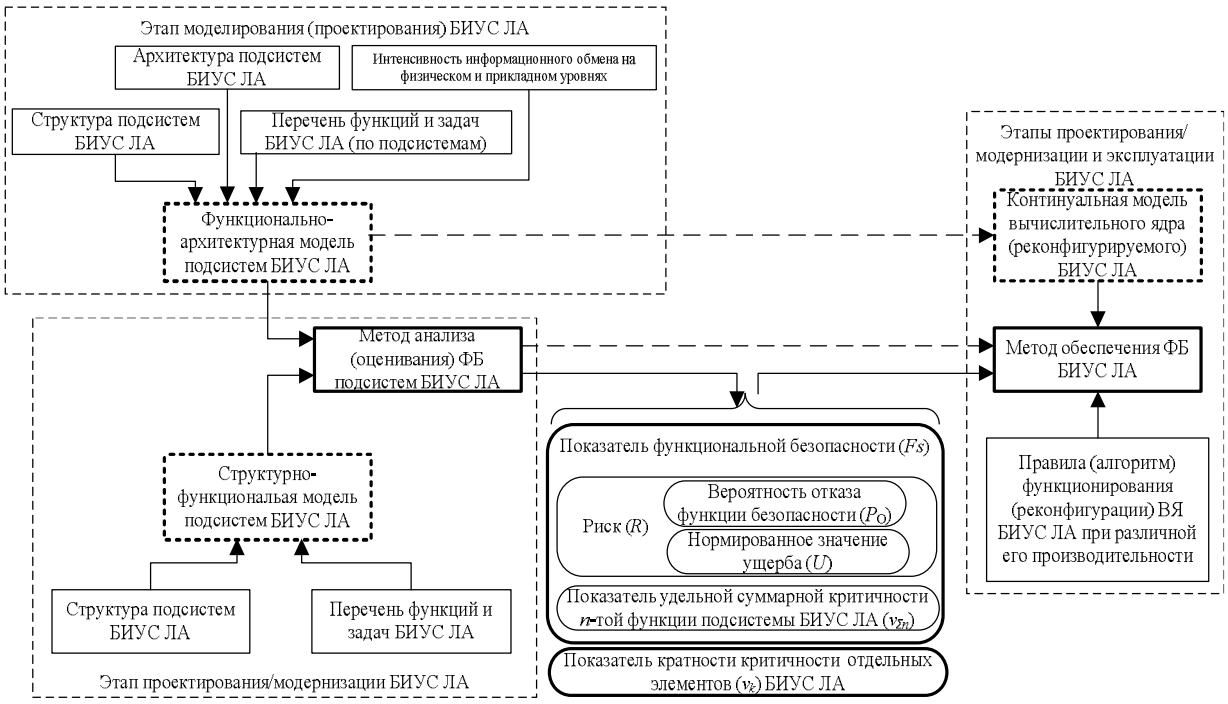

Рис. 1. Методологический аппарат анализа, оценивания и поддержания функциональной безопасности БИУС ЛА.

Метод оценивания ФБ БИУС ЛА с использованием структурной и функционально-архитектурной модели БИУС ЛА позволяет осуществить качественную и количественную оценку указанного свойства с помощью комплексного показателя функциональной безопасности (Fs), который определяется удельной суммарной критичностью n-той функции безопасности ($F_Б$) - $\nu_{\Sigma n}$; показателем риска, связанного с данной $F_Б$ - R_n, который в свою очередь зависит от вероятности отказа n-той $F_Б$ - P_{on}, и ущерба, возможного при отказе данной $F_Б$ - U_n [1]. В отличие от существующих, данный метод учитывает структурную надежность соответствующих подсистем БИУС ЛА (вероятность отказа функции безопасности - P_o) и функциональную критичность ее отдельных элементов (показатель кратности критичности - ν_k) для выполнения $F_Б$ БИУС ЛА [1]. Данный метод может применяться на этапе проектирования или модернизации БИУС ЛА, а также на этапе моделирования ее функционирования для исследования надежности и ФБ [2].

Метод обеспечения ФБ БИУС ЛА на этапах её проектирования и эксплуатации, использует функционально-архитектурную модель БИУС ЛА с реконфигурируемым ВЯ (континуальная модель) и учитывает степени критичности отдельных элемен-

тов структурно-функциональной схемы БИУС ЛА (метод анализа (оценивания) ФБ подсистем БИУС ЛА) [2, 3].

Данный метод также может использоваться на этапе эксплуатации для оптимизации проведения реконфигурации информационно-вычислительных (информационно-управляющих) процессов функциональных подсистем по результатам оперативного контроля критичности и ФБ отдельных функционально-информационных потоков с применением правил функционирования ВЯ БИУС ЛА при различной его производительности [4].

3. Описание функционально-архитектурной модели БИУС ЛА

С помощью приведенной в [4] функционально-архитектурной модели БИУС ЛА можно описать распределение ограниченных вычислительных ресурсов (ВР) ВМ для обеспечения выполнения $F_Б$ с поддержанием их заданного уровня надежности (см. рис. 2) [5].

Совокупный ВР БИУС ЛА в данном случае рассматривается как сумма ВР одного типа (BM_1, … BM_N), но разного объема и надежности.

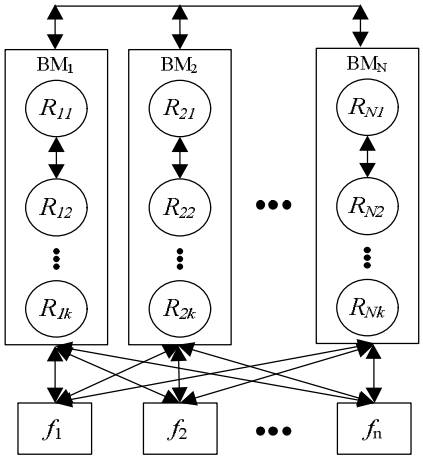

Рис. 2. Распределение ограниченных вычислительных ресурсов ВМ

Для описания распределения конкретных ВР введем необходимые обозначения:

– f_i – функции безопасности, выполнение которых обеспечивается функционированием БИУС ЛА (i = 1,..., n);

– m_j – количество вычислительных ресурсов BM_j (j = 1,..., N);

– R_{jk} – k-тый ВР для BM_j (j = 1,..., N; k = 1,..., m_j);

– r_{jk} – производительность k-того ВР в BM_j (j = 1,..., N; k = 1,..., m_j);

– p_{jk} – показатель надежности ВР R_{jk} в BM_j (j = 1,..., N; k = 1,..., m_j);

– z_{ij} – потребность $F_Б$ в вычислительных ресурсах BM_j, а именно z_{ij} соответствует необходимой совокупной производительности ВР R_{jk} для выполнения $F_Б$ f_i (имеет значение 0 если ВР не нужен);

– $P_{задi}$ – заданные значения показателей надежности $F_Б$ f_i;

– e_{ijk} – параметр определяющий возможность обеспечения $F_Б$ f_i k-тым ВР R_{jk}:

$$e_{ijk} = \begin{cases} 1, \text{ если } f_i \text{ может быть обеспечена } R_{jk}, \\ 0, \text{ в противном случае.} \end{cases}$$

– y_{ijk} – переменная определяющая закрепление реального ВР R_{jk} за $F_Б$ f_i для обеспечения её функционирования:

$$y_{ijk} = \begin{cases} 1, \text{ если } R_{ik} \text{ закрепляется за } f_i, \\ 0, \text{ в противном случае} \end{cases}$$

– x_i – переменная, определяющая выполнение $F_Б$ f_i:

$$x_i = \begin{cases} 1, \text{ если } f_i \text{ выполняется,} \\ 0, \text{ в противном случае} \end{cases}$$

– d_{ij} – параметр, определяющий потребность $F_Б$ f_i в ВР R_{jk}:

$$\begin{cases} d_{ij} = 1, \text{ если } z_{ij} \neq 0, \\ d_{ij} = 0, \text{ если } z_{ij} = 0 \end{cases}.$$

Закрепление ВР за определенной $F_Б$ определяется выражением:

$$\sum_{k=1}^{m_j} e_{ijk} \cdot y_{ijk} = d_{ij} \cdot x_i \,. \qquad (1)$$

Выражение (1) показывает, что каждая потребность в ВР d_{ij} рассматриваемой $F_Б$ f_i должна быть удовлетворена одним из ВР R_{jk}, если таковой может быть использован для выполнения данной $F_Б$. В данном случае имеет место ресурсное ограничение:

$$\sum_{i=1}^{n} y_{ijk} \cdot p_{ij} \le r_{jk} \,. \qquad (2)$$

Рассмотрим случай, когда $F_Б$ обеспечивается в полном объеме только при условии наличия всех необходимых для ее выполнения ВР. Тогда для оценки надежности выполнения $F_Б$, используем последовательную структурную схему надежности, при которой показатель надежности (например, вероятность безотказной работы) рассчитывается как результат умножения показателей надежности каждого из компонентов (вероятностей безотказной работы используемых ресурсов R_{jk} - p_{jk}) по формуле:

$$P = \prod_{k=1}^{m_j} p_{jk} \,, \qquad (3)$$

где P – показатель надежности $F_Б$; p_{jk} – вероятность безотказной работы ВР R_{jk}, предоставленного j-ым ВМ.

При этом для отдельной $F_Б$ f_i рассчитываемый показатель надежности P должен быть не меньше заданного показателя надежности $P_{зад\ i}$.

Чтобы уйти от операции умножения в (3), преобразуем обе части выражения:

$$\ln P = \sum_{k=1}^{m_j} \ln p_{jk} . \qquad (4)$$

Учитывая только ВР, которые задействованы для выполнения конкретной $F_Б$ f_i, требование к вероятности безотказной работы при распределении ВР ВМ будет иметь вид:

$$\sum_{j=1}^{N} \sum_{k=1}^{m_j} y_{ijk} \cdot \ln p_{jk} \geq \ln p_{задi}, \text{ при } i = \overline{1,n}. \qquad (5)$$

Если рассматривать x_i и y_{ijk} как переменные, то задача (1), (2), (5) является задачей булевого программирования и может быть решена соответствующими методами [6].

Данный подход позволяет с одной стороны осуществлять распределение ВР БИУС ЛА для обеспечения выполнения функций безопасности при заданном уровне надежности, а с другой - более точно изучать порядок взаимодействия элементов, входящих в архитектурные модели систем данного класса. При этом у представленной функционально-архитектурной модели есть ограничения, связанные с тем, что при рассмотрении порядка функционирования отдельных элементов архитектуры БИУС ЛА и её подсистем остаются неучтенными сбои (ошибки) в работе операционного ПО и отдельных прикладных ПС, влияющих на точность вычислений, а следовательно, и на конечные решения - формируемые управляющие сигналы, что может стать следствием проявления не выявленных на этапах верификации и валидации дефектов проектирования ПО либо БИУС в целом и причиной появления новых дефектов (в том числе взаимодействия отдельных элементов архитектуры), что может приводить к значительному снижению уровня функциональной безопасности оцениваемых систем (подсистем).

В результате, для проведения оценивания ФБ БИУС ЛА целесообразным является применение как вышеизложенных подходов к моделированию, так и построение моделей надежности функционирующих систем с учетом новых видов дефектов взаимодействия их элементов и структурных особенностей их построения и архитектурной реконфигурации.

Выводы

В статье предоставлен подход к созданию методологического аппарата анализа, оценивания и обеспечения функциональной безопасности бортовых информационно-управляющих систем летательных аппаратов, основанный на ранее разработанных моделях и методах, с помощью которого на различных этапах жизненного цикла БИУС ЛА возможно проведение оценивания и прогнозирования возможных вариантов функционирования БИУС ЛА с поддержанием заданного уровня их функциональной безопасности.

Для обеспечения полноты описания функционирования БИУС ЛА предложено использование соответствующих функционально-архитектурных моделей, позволяющее в процессе обеспечения функциональной безопасности данного объекта осуществлять распределение вычислительных ресурсов для выполнения функций безопасности с заданной надежностью учитывая порядок взаимодействия всех входящих в них элементов, при функционировании.

Литература

1. Похил, В.С. Удосконалений метод аналізу й оцінювання функціональної безпеки бортових інформаційно-керуючих систем повітряного судна [Текст] / В.С. Похил // Системи озброєння і військова техніка. – Х.: Харківський ун-т Повітряних Сил ім. Івана Кожедуба, 2010. – № 2 (22). – С. 136 – 142.

2. Похил, В.С. Удосконалений метод та інформаційна технологія забезпечення функціональної безпеки бортових інформаційно-керуючих систем авіації на етапі проектування [Текст] / В.С. Похил // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: Харківський ун-т Повітряних Сил ім. Івана Кожедуба, 2010. – № 2 (4). – С. 65 – 70.

3. Похил, В.С. Метод забезпечення функціональної безпеки бортових інформаційно-керуючих систем літальних апаратів на етапі їх експлуатації [Текст] / В.С. Похил // Системи озброєння і військова техніка. – Х.: Харківський ун-т Повітряних Сил ім. Івана Кожедуба, 2010. – № 3 (23). – С. 68 – 74.

4. Похил, В.С. Модели и методы обеспечения функциональной безопасности бортовых информационно-управляющих систем летательных аппаратов на разных этапах их жизненного цикла [Текст] / Похил В.С. // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2011. – № 2 (18). – С. 142 – 151.

5. Теленик, С.Ф. Моделі управління розподілом обмежених ресурсів в інформаційно-телекомунікаційній мережі АСУ [Текст] / С.Ф. Теленик, О.І. Ролік, М.М. Букасов // Вісник Національного технічного університету України «КПІ»: Інформатика, управління та обчислювальна техніка. — 2006.— № 44. — С. 234 — 239.

6. Зайченко, Ю.П. Исследование операций [Текст] / Ю.П. Зайченко. – 6-е изд., перераб. и доп. – К.: Издательский Дом «Слово», 2003. – 688 с.

Поступила в редакцию 1.02.2012

Рецензент: д-р техн. наук, проф., зав. кафедры В.А. Краснобаев, Полтавский национальный технический университет им. Юрия Кондратюка, Полтава, Украина.

МЕТОДИ АНАЛІЗУ, ОЦІНЮВАННЯ ТА ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ БОРТОВИХ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ ЛІТАЛЬНИХ АПАРАТІВ НА ОСНОВІ ФУНКЦІОНАЛЬНО-АРХІТЕКТУРНОГО МОДЕЛЮВАННЯ

В.С. Похил, О.В. Харибін

Розглядається підхід до створення методологічного апарату аналізу, оцінювання та забезпечення функціональної безпеки авіаційних бортових інформаційно-керуючих систем на основі раніше розроблених моделей і методів, що дозволяють на ранніх етапах життєвого циклу БІУС ЛА проводити оцінювання та прогнозування можливих варіантів функціонування БІУС ЛА з підтриманням заданого рівня їх функціональної безпеки. Пропонується використовувати функціонально-архітектурні моделі при обґрунтуванні розподілу обчислювальних ресурсів бортових інформаційно-керуючих систем по підсистемам, що входять в її склад, з урахуванням необхідного рівня надійності та функціональної безпеки.

Ключові слова: метод, функціональна безпека, функціонально-архітектурна модель, бортова інформаційно-керуюча система.

METHODS OF THE AIRCRAFTS ON-BOARD INSTRUMENTATION & CONTROL SYSTEMS FUNCTIONAL SAFETY ANALYSIS, ASSESSMENT AND SUPPORT BASED ON THE FUNCTIONAL-ARCHITECTURAL MODELING

V.S. Pokhyl, A.V. Kharybin

An approach to the development of the aircrafts on-board instrumentation & control systems functional safety analysis, assessment and support methodology, which is based on the previously developed models and methods, is described, allowing to hold CICS estimation and forecasting options CICS operation of aircraft while maintaining a given level of functional safety on the early stages of the life cycle of the aircraft. It is proposed to use the functional-architectural models to justify the allocation of computing resources of the aircraft on-board instrumentation & control system within their subsystems in accordance with the required level of their reliability and functional safety.

Key words: method, functional safety, functional-architectural model, on-board instrumentation & control system.

Похил Виктория Станиславовна – соискатель, старший научный сотрудник отдела технической аналитики и управления проектами ПАО «НПП «Радий», Кировоград, Украина.

Харыбин Александр Викторович – канд. техн. наук, начальник отдела технической аналитики и управления проектами ПАО «НПП «Радий», Кировоград, Украина.